





Apex

С

C++

CloudFormation

COBOL

C#

CSS

Flex

Go

5 **HTML**

Java

JavaScript

Kotlin

Kubernetes

Objective C

PHP

PL/I

PL/SQL

Python

RPG

Ruby

Scala

Swift

Terraform

Text

TypeScript

T-SQL

VB.NET

VB₆

XML



HTML static code analysis

Unique rules to find Bugs, Security Hotspots, and Code Smells in your HTML code

₩ Bug (24) All rules (65)

Security Hotspot (3)

Code Smell 38

Using HTML comments is

security-sensitive

Tags

cwe jsp-jsf owasp

Analyze your code

Search by name...

Using HTML-style comments in a page that will be generated or interpolated server-side before being served to the user increases the risk of exposing data that should be kept private. For instance, a developer comment or line of debugging information that's left in a page could easily (and has) inadvertently expose:

- · Version numbers and host names
- Full, server-side path names
- · Sensitive user data

Every other language has its own native comment format, thus there is no justification for using HTML-style comments in anything other than a pure HTML or XML file.

Ask Yourself Whether

- The comment contains sensitive information.
- The comment can be removed.

Recommended Secure Coding Practices

It is recommended to remove the comment or change its style so that it is not output to the client.

Sensitive Code Example

< % out.write("<!-- \${username} -->"); // Sensitive %> <!-- <% out.write(userId) %> --> // Sensitive <!-- #{userPhone} --> // Sensitive <!-- \${userAddress} --> // Sensitive <!-- Replace 'world' with name --> // Sensitive <h2>Hello world!</h2>

Compliant Solution

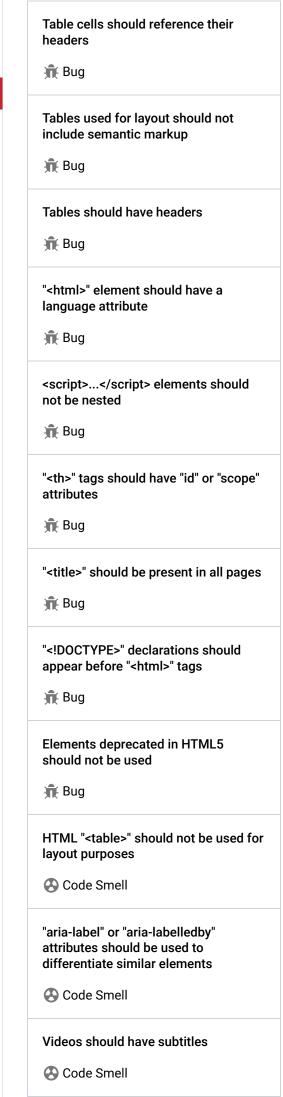
<%-- Replace 'world' with name --%> $\ // \$ Compliant <h2>Hello world!</h2>

See

- OWASP Top 10 2017 Category A3 Sensitive Data Exposure
- MITRE, CWE-615 Information Exposure Through Comments

Available In:





© 2008-2022 SonarSource S.A., Switzerland. All content is copyright protected. SONAR, SONARSOURCE, SONARLINT, SONARQUBE and SONARCLOUD are trademarks of SonarSource S.A. All other trademarks and copyrights are the

property of their respective owners. All rights are expressly reserved. $\underline{\text{Privacy Policy}}$

Attributes deprecated in HTML5 should not be used Code Smell
Sections of code should not be commented out Code Smell
Track uses of "FIXME" tags Code Smell
Meta tags should not be used to refresh or redirect Code Smell
Links should not directly target images Code Smell
" " and "" tags should be used ••• Bug
" "and "<dt>" item tags should be in "", "" or "<dl>" container tags</dl></dt>
Server-side image maps ("ismap" attribute) should not be used
" <frames>" should have a "title" attribute</frames>